Abelian Groups

A group is Abelian if $xy = yx$ for all group elements x and y.

The basis theorem

An Abelian group is the direct product of cyclic $p-$groups. This direct product decomposition is unique, up to a reordering of the factors.

Proof: Let $n = p_1^{n_1} \cdots p_k^{n_k}$ be the order of the Abelian group G, with p_i's distinct primes. By Sylow's theorem it follows that G has exacly one Sylow $p-$subgroup for each of the k distinct primes p_i. Consequently G is the direct product of its Sylow $p-$subgroups. [We call the Sylow $p-$subgroups the $p - primary$ parts of G.] It remains to show that an Abelian $p-$group (corresponding to a $p-$primary part of G) is the direct product of cyclic groups.

We prove this by induction on the power m of the order p^m of the $p-$group. Assume that the result is true for m. Let P be an Abelian group of order p^{m+1} and Q a subgroup of P of order p^m (such Q exists by Sylow's theorem). By induction $Q =< a_1 > \times < a_2 > \times \cdots \times < a_r >$ with

$$| < a_i > | = p^{k_i}, \quad k_1 \geq k_2 \geq \cdots \geq k_r, \quad \sum_{i=1}^{r} k_i = m.$$

Let $a \in P - Q$. Then $a^p \in Q$ and therefore $a^p = a_1^{s_1} a_2^{s_2} \cdots a_r^{s_r}$. Taking $b = a a_1^{t_1} a_2^{t_2} \cdots a_r^{t_r}$ for suitable t_i, we obtain $b \in P - Q$, and $b^p = a_1^{d_1} a_2^{d_2} \cdots a_r^{d_r}$, where for each i either $d_i = 0$ or $(d_i, p) = 1$. [Take a deep breath and convince ourself that such b exists.]

If all the d_i are 0, then $b^p = 1$ and, by a cardinality argument, $P =< a_1 > \times < a_2 > \times \cdots \times < a_r > \times < b >$.

If not, let j be the first index for which $d_j \neq 0$; hence $| < b > | = p^{k_j+1}$. We show that $P =< a_1 > \times \cdots \times < a_{j-1} > \times < b > \times < a_{j+1} > \times \cdots \times < a_r >$. To prove this it suffices to show that

$$< b > \cap (< a_1 > \times \cdots \times < a_{j-1} > \times < a_{j+1} > \times \cdots \times < a_r >) = 1,$$

or that

$$b^{p^{k_j}} \notin < a_1 > \times \cdots \times < a_{j-1} > \times < a_{j+1} > \times \cdots \times < a_r >,$$

since every nontrivial subgroup of $< b >$ contains $b^{p^{k_j}}$. However, from the choice of b we see that $b^{p^{k_j}}$ contains in its decomposition $a_j^{d_j p^{k_j - 1}}$ which is different from 1 because $(d_j, p) = 1$. It follows that

$$b^{p^{k_j}} \notin < a_1 > \times \cdots \times < a_{j-1} > \times < a_{j+1} > \times \cdots \times < a_r >,$$

and this shows that P is the direct product of cyclic groups.

To see that this direct product decomposition is unique, it suffices to show that it is unique for each of the $p-$primary parts. Indeed, if p^{m_1} is the highest order of an element in P, then any direct product decomposition necessarily contains a cyclic group of order p^{m_1} as a direct factor. The factor group of P to this cyclic subgroup is of lesser order than P, and the uniqueness of its factors follows by induction. This ends the proof.

A consequence of the above result is that if $(x_1, \ldots, x_s)$ are the generators of the cyclic direct factors of the Abelian group G, then any element $x \in G$ can be written uniquely as $x = x_1^{j_1} \cdots x_s^{j_s}$, for positive integers j_i. We say that $(x_1, \ldots, x_s)$ is a *basis* for G. The orders of the basis elements x_i are the *invariants* of G.

For an Abelian $p-$group P of order p^m with invariants $p^{m_1} \geq \cdots \geq p^{m_k}$ we call the vector $(m_1, \ldots, m_k)$ of positive integers $m_1 \geq \cdots \geq m_k$, which satisfy $\sum m_i = m$, the *type* of P. The type of P is a *partition* of m. Examining the extremes, a group of type m is cyclic of order p^m, while a group of type (1, 1, ... , 1) is a direct product of m cyclic groups each of order p. We call the latter group *elementary Abelian.*

Graphically represent the type of P by k rows of dots, the first of which contains m_1 dots, the second m_2 dots, and so on; we call this graph the *Ferrer diagram* of P. Flip the Ferrer diagram in its main diagonal. What results is another Ferrer diagram with s_i dots in row i. We call the vector $(s_1, s_2, \ldots)$ the *signature* of P. [For example, if the type is (4, 2, 1), then the signature is (3, 2, 1, 1).] It is occasionally helpful to see the type and signature as vectors of infinite lengths with all but the first finitely many entries being zero.

In view of the Basis Theorem proved above, it is clear that *there is a bijection between the nonisomorphic Abelian p-groups of order* p^m *and the partitions of* m.

There are, therefore, as many Abelian $p-$groups of order p^m as there are partitions of m. A determination in "closed form" of the number of such partitions was made by Hardy and Ramanujan by a process called the "circle method". On the other hand, recurrences for such partitions can easily be found.

!!!Include Delsarte's result here

Composition series

A *subnormal series* of a group G is a sequence of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_n$ such that G_{i+1} is normal in G_i, for $0 \leq i < n$. The *factors* of the series are the quotient groups G_i/G_{i+1}. By the *length* of a series we understand the number of strict inclusions that occur in the series (or, equivalently, the number of nonidentity factors).

If each of the groups that occur in a subnormal series are normal in G we call the series *normal*.

A *one term refinement* of a subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_n$ is a subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_i \geq H \geq G_{i+1} \geq \cdots \geq G_n$ or a subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_n \geq H$; the subgroup H is the inserted term. A *refinement* of a subnormal series is a subnormal series obtained by succesively performing a finite number of one term refinements. Note that a refinement may contain more terms than the original series without having greater length. This happens if the groups that are inserted are repetitions of groups already in the series.

A subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$ is a *composition series* if each factor G_i/G_{i+1} is a simple group.

Two subnormal series are *equivalent* if there is a bijective correspondence between the nonidentity factors of the two series such that the corresponding factors are isomorphic groups. [In particular, equivalent series must necessarily have the same length.]

Lemma (Zassenhaus)

If $A_1 \trianglelefteq A$ and $B_1 \trianglelefteq B$ are subgroups of a group G, then

(a) $A_1(A \cap B_1)$ is normal in $A_1(A \cap B)$

(b) $B_1(A_1 \cap B)$ is normal in $B_1(A \cap B)$

(c) $\frac{A_1(A\cap B)}{A_1(A\cap B_1)} \cong \frac{B_1(A\cap B)}{B_1(A_1\cap B)}$.

Proof: Observe that $B_1 \trianglelefteq B$ implies that $A \cap B_1 = (A \cap B) \cap B_1$ is normal in $A \cap B$. Similarly $(A_1 \cap B) \trianglelefteq (A \cap B)$. It follows that $D = (A_1 \cap B)(A \cap B_1)$ is a normal subgroup of $A \cap B$.

Define $f : A_1(A \cap B) \to (A \cap B)/D$ as follows. For $a \in A_1$ and $c \in A \cap B$ let $f(ac) = cD$. The function f is a well-defined surjective homomorphism. [Indeed, $f((a_1c_1)(a_2c_2)) = f(a_1a_3c_1c_2) = c_1c_2D = (c_1D)(c_2D) = f(a_1c_1)f(a_2c_2)$, where $a_i \in A_1$, $c_i \in A \cap B$, and $c_1a_2c_1^{-1} = a_3$ since $A_1 \trianglelefteq A$.] The kernel of f is $\ker f = A_1(A \cap B_1)$. This shows that $A_1(A \cap B_1)$ is normal in $A_1(A \cap B)$ and, by the First Isomorphism Theorem, $\frac{A_1(A\cap B)}{A_1(A\cap B_1)} \cong \frac{A\cap B}{D}$.

An entirely parallel argument yields $\frac{B_1(A\cap B)}{B_1(A_1\cap B)} \cong \frac{A\cap B}{D}$. The isomorphism written in (c) now follows. This concludes the proof.

And now, a fundamental Theorem of Schreier.

Theorem (Schreier)

Any two subnormal series of a group have subnormal refinements that are equivalent.

Proof: Take two subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_n$ and $G = H_0 \geq H_1 \geq \cdots \geq H_m$. Append each with 1, that is, define $G_{n+1} = H_{m+1} = 1$. Consider the groups

$G_i = G_{i+1}(G_i \cap H_0) \geq \cdots \geq G_{i+1}(G_i \cap H_j) \geq \cdots \geq G_{i+1}(G_i \cap H_{m+1}) = G_{i+1}$, for each $0 \leq i \leq n$. The Zassenhaus Lemma applied to $G_{i+1} \trianglelefteq G_i$ and $H_{j+1} \trianglelefteq H_j$ shows that $G_{i+1}(G_i \cap H_{j+1})$ is normal in $G_{i+1}(G_i \cap H_j)$, for each $0 \leq j \leq m$. Inserting the above groups between G_i and G_{i+1}, and denoting $G_{i+1}(G_i \cap H_j)$ by G_{ij}, yields a subnormal refinement of $G = G_0 \geq G_1 \geq \cdots \geq G_n$. Specifically,

$G = G_{00} \geq \cdots \geq G_{0m} \geq G_{10} \geq \cdots \geq G_{1m} \geq \cdots \geq G_{n0} \geq \cdots \geq G_{nm}$, where $G_{i0} = G_i$. A parallel argument yields a refinement of $G = H_0 \geq H_1 \geq \cdots \geq H_m$, specifically,

$G = H_{00} \geq \cdots \geq H_{n0} \geq H_{01} \geq \cdots \geq H_{n1} \geq \cdots \geq H_{0m} \geq \cdots \geq H_{nm}$, where $H_{ij} = H_{j+1}(G_i \cap H_j)$ and $H_{0j} = H_j$. Both refinements have $(n+1)(m+1)$ not necessarily distinct terms. For each (i, j), the Zassenhaus Lemma applied to $G_{i+1} \trianglelefteq G_i$ and $H_{j+1} \trianglelefteq H_j$ yields the isomorphism:

$$\frac{G_{ij}}{G_{i,j+1}} = \frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})} \cong \frac{H_{j+1}(G_i \cap H_j)}{H_{j+1}(G_{i+1} \cap H_j)} = \frac{H_{ij}}{H_{i+1,j}}.$$

This provides the bijective correspondence on factors, proving the equivalence of the two subnormal series.

Note: An analogous result can be obtained for normal series in a similar manner.

Let us examine Schreier's Theorem in the case of composition series. Since the factors of a composition series are simple groups, it follows that any refinement of a composition series is equivalent to that series. Schreier's Theorem, therefore, implies that two composition series are necessarily equivalent. This result is stated below.

Theorem (Jordan-Hölder)

Any two composition series of a group are equivalent.

The Jordan-Hölder Theorem tells us that a group G determines a unique list of simple groups as the factors of any of its composition series. We call the nonidentity factors of any composition series the *composition factors* of the group. These simple groups provide valuable information about G, though they clearly do not determine G up to isomorphism. [Indeed, the symmetric group S_3 and the Abelian group $Z_3 \times Z_2$ are nonisomorphic groups having the same factors of respective composition series.]

Characteristic Subgroups

A subgroup H of a group G is *characteristic* in G if H is left invariant by all the automorphisms of G. We write HcG to indicate that H is characteristic in G. A characteristic subgroup is certainly normal, since conjugations form a subgroup of the automorphism group.

It is easy and not unpleasant to verify the following properties of characteristic subgroups:

- HcK *and* $KcG \Rightarrow HcG$
- HcK *and* $K \trianglelefteq G \Rightarrow H \trianglelefteq G$
- HcG *and* $KcG \Rightarrow (HK)cG$ *and* $(H \cap K)cG$.

A group G is *characteristically simple* if G and 1 are its only characteristic subgroups. A *minimal normal subgroup* of G is a minimal member of the set of nonidentity normal subgroups of G, partially ordered by inclusion. [The second property listed above tells us, in particular, that *minimal normal subgroups are characteristically simple.]*

$*$ *If* $1 \neq G$ *is a characteristically simple group, then* G *is the direct product of isomorphic simple groups.*

Proof: Let H be a minimal normal subgroup of G. Consider the set of subgroups $S = \{f(H) : f \in Aut(G)\}$; denote the elements of the set S by $H = H_1, H_2, \ldots, H_n$. The subgroups H_i are normal in G, and $H_i \cap H_j = 1$ for all $i \neq j$. [Indeed, they all are minimal normal subgroups of G since

$$f(H)^x = xf(H)x^{-1} = f(y)f(H)f(y^{-1}) = f(yHy^{-1}) = f(H),$$

which shows that $Aut(G)$ acts on the normal subroups of G. The subgroup $H_i \cap H_j$ is normal in G and a proper subgroup of the minimal subgroup H_i, thus equal to 1.] We conclude that $< S >= H_1 \times \cdots \times H_n$. Since $H \leq < S >$ and $< S >$ is characteristic in G, by the assumed characteristic simplicity of G we have $G =< S > (= H_1 \times \cdots \times H_n)$.

We can now see that H must be simple; for if $1 \neq K \trianglelefteq H$, then $H \leq N_G(K)$ and also $H_i \leq N_G(K)$, since $G = H_1 \times \cdots \times H_n$ and thus elements of H_i commute with elements of H (and thus of K) for all $i = 2, \ldots, n$. This concludes the proof.

Specializing the result to Abelian groups, we immediately conclude that *a characteristically simple Abelian group is elementary Abelian.*

Commutators

The *commutator* of x and y is the group element $xyx^{-1}y^{-1}$, which we denote by $[x, y]$. For $X, Y \leq G$ define

$$[X, Y] = < [x, y] : x \in X, y \in Y > .$$

Furthermore, for $z \in Z \leq G$ write $[x, y, z]$ for $[[x, y], z]$ and $[X, Y, Z]$ for $[[X, Y], Z]$.

$*$ *If $a, b, c \in G$ and $X, Y \leq G$, then*

(1) $[a, b] = 1$ if and only if $ab = ba$.

(2) $[X, Y] = 1$ if and only if $xy = yx$ for all $x \in X$ and $y \in Y$.

(3) If f is a group homomorphism, then $f([a, b]) = [f(a), f(b)]$ and $f([X, Y]) = [f(X), f(Y)]$.

(4) $[ba, c] = [a, c]^b[b, c]$ and $[b, ac] = [b, a][b, c]^a$. (5) $X \leq N_G(Y)$ if and only if $[X, Y] \leq Y$.

(6) $[X, Y] = [Y, X] \trianglelefteq G$.

Statements (1), (2), and (3) are immediate. Assertion (4) involves streightforward verification. To see (5), let $X \leq N_G(Y)$; then $xyx^{-1} \in Y$, and therefore $xyx^{-1}y^{-1} \in Y$. Conversely, assume that $[X, Y] \leq Y$; then $xyx^{-1}y^{-1} \in Y$, and therefore $xyx^{-1} \in Y$, showing that $X \leq N_G(Y)$.

As to (6), notice that $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$, telling us that $[X, Y] = [Y, X]$. To prove normality of $[X, Y]$ in $< X, Y >$ it suffices to show that $[x, y]^z \in [X, Y]$ for $z \in X \cup Y$. Furthermore, since $[x, y]^{-1} = [y, x]$ it suffices to restrict $z \in X$. If so, by the first equation in (4) we have $[x, y]^z = [zx, y][z, y]^{-1} \in [X, Y]$, and the proof is complete.

The *commutator* (or *derived*) subgroup of G is $G^{(1)} = [G, G]$. Recursively define $G^{(n+1)} = [G^{(n)}, G^{(n)}]$, for $n \geq 1$. Let also $G^{(0)} = G$.

$*$ *If G is a group and $H \leq G$, then*

(1) $H^{(n)} = G^{(n)}$

(2) If f *is a surjective homomorphism, then* $f(G^{(n)}) = (f(G))^{(n)}$

(3) $G^{(n)}$ *is characteristic in* G

(4) $G^{(1)} \leq H$ *if and only if* $H \trianglelefteq G$ *and* G/H *is Abelian*

Solvable groups

A group is *solvable* if it possesses a subnormal series $G_0 \geq G_1 \geq \cdots \geq G_m = 1$ whose factors are Abelian.

∗ *A group* G *is solvable if and only if* $G^{(n)} = 1$ *for some integer* n*.*

If $G^{(n)} = 1$, then $G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(n)} = 1$ is a subnormal series (a normal series, in fact) with Abelian factors. [The factors are indeed Abelian, by (4) of the previous result.] Conversely, assume that $G = G_0 \geq G_1 \geq \cdots \geq G_m = 1$ is a subnormal series with G_i/G_{i+1} Abelian. Then, by (4) above, $G^{(1)} \leq G_1$, $G^{(2)} = [G^{(1)}, G^{(1)}] \leq [G_1, G_1] \leq G_2$ and, proceeding inductively, $G^{(i)} \leq G_i$, for all $1 \leq i \leq m$. It follows that $G^{(m)} \leq G_m = 1$.

Let G be solvable with $G^{(n)} = 1$. Then $G^{(i+1)} < G^{(i)}$, with strict inclusion for $i < n$; [else $G^{(n)}$ can never be 1]. In particular $G^{(1)} < G$.

∗ *A group is solvable if and only if all its composition factors are of prime order.*

Indeed, if G is solvable with $G = G_0 \geq G_1 \geq \cdots \geq G_m$ a subnormal series, then the composition factors of the Abelian groups G_i/G_{i+1} are necessarily (Abelian) of prime order. By taking the preimages of all these intermediate groups we obtain a composition series of G with factors of prime order. The converse is trivial, since groups of prime order are Abelian.

$*$ *Subgroups and homomorphic images of solvable groups are solvable.*

Let G be solvable with $G^{(n)} = 1$. If $H \leq G$, then $H^{(n)} \leq G^{(n)} = 1$, proving that H is solvable. We also know that $f(G)^{(n)} = f(G^{(n)}) = f(1) = 1$, for any homomorphism f.

$*$ *If $H \trianglelefteq G$ and H and G/H are solvable, then G is solvable.*

Solvability of G/H implies the existence of a subnormal series whose preimage in G remains a subnormal series with Abelian factors that ends in H. Extend this series with the commutator subgroups $H^{(i)}$ of H, which ends in 1. What results is a subnormal series of G with Abelian factors, proving the solvability of G.

$*$ *Solvable minimal normal subgroups are elementary Abelian.*

If M is such a subgroup of a group G, then $M^{(1)} = 1$, since by solvability of M the subgroup $M^{(1)}$ is a strict characteristic subgroup of M, and thus normal in G. The fact that $M^{(1)} = 1$ implies that M is Abelian. As an Abelian minimal normal subgroup, M is the direct product of isomorphic (simple) groups of prime order. Thus M is elementary Abelian.

Nilpotent groups

Define $L_0(G) = G$, and recursively $L_{i+1}(G) = [L_i(G), G]$, for $i \geq 0$. A group G is said to be *nilpotent* if $L_n(G) = 1$ for some n. The *class* of a nilpotent group is m, where $m = min\{i : L_i(G) = 1\}$.

Observe that $G^{(i)} \leq L_i(G)$ for all i, and therefore $G^{(n)} = 1$ if $L_n(G) = 1$. This tells us that

$*$ *Nilpotent groups are solvable.*

The *center* of a group G is $Z(G) = \{x \in G : [x, y] = 1$, for all $y \in G\}$. It is easy to see that $Z(G)$ *is characteristic in* G.

$*$ *The subgroups* $L_n(G)$ *have the following properties:*

(1) $L_n(G)$ *is characteristic in* G*, for all* n

(2) $L_{n+1}(G) \leq L_n(G)$

(3) $L_n(G)/L_{n+1}(G) \leq Z(G/L_{n+1}(G))$

Part (1) follows from (3) in the commutator section and induction on n. Part (1) above and part (5) in the commutator section imply (2). Part (3) follows from (1) and (3) in the commutator section.

Let $Z_0(G) = 1$ and recursively define $Z_{i+1}(G)$ to be the preimage in G of $Z(G/Z_i(G))$, for $i \geq 0$. Evidently $Z_n(G)$ is characteristic in G, since HcG and $(K/H)c(G/H)$ imply KcG.

$*$ *A group* G *is nilpotent if and only if* $G = Z_n(G)$*, for some* n*. If* G *is nilpotent, then the class of* G *is* $m = min\{n : G = Z_n(G)\}$.

Assume that G is nilpotent of class m. Using induction we show that $L_{m-i}(G) = Z_i(G)$. For $i = 0$ this means $L_m(G) = Z_0(G)$, both being 1 (by assumption and definition, respectively). Assume that $L_{m+1-i}(G) \leq Z_{i-1}(G)$. Then $[L_{m-i}(G), G] = L_{m+1-i}(G) \leq Z_{i-1}(G)$, which tells us that $[L_{m-i}(G)/Z_{i-1}(G), G/Z_{i-1}(G)] = \bar{1}$, where $\bar{1} = Z_{i-1}(G)$. We conclude that $L_{m-i}(G)/Z_{i-1}(G) \leq Z(G/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G)$, which shows that $L_{m-i}(G) \leq Z_i(G)$. This proves that $L_{m-i}(G) \leq Z_i(G)$, for all i. In particular, $Z_m(G) = L_0(G) = G$. It allows us to conclude also that $min\{n : G = L(G)\}$ is less than or equal to the class of G.

Conversely, assume that $Z_k(G) = G$, for some k. Inductively we show that $L_i(G) \leq Z_{k-i}(G)$, for all i. The inclusion is true for $i = 0$. Assume that $L_{i-1}(G) \leq Z_{k-i+1}(G)$. We have $L_i(G) = [L_{i-1}(G), G] \leq [Z_{k-i+1}(G), G] \leq Z_{k-i}(G)$, by (5) in the commutator section. In particular, $L_k(G) \leq Z_0(G) = 1$. This shows that the class of G is less than or equal to $min\{n : G = Z_n(G)\}$. End of proof.

By examining the series $Z_j(G)$, the following statement follows immediately from the previous result:

$*$ *A group* $1 \neq G$ *is nilpotent of class m if and only if G/Z(G) is nilpotent of class m-1.*

Let us quickly examine the state of nilpotency for $p-$groups.

$*$ *All p-groups are nilpotent.*

Let P be a $p-$group. Observe first that the center $Z(P) \neq 1$. Indeed, let P act on itself by conjugation. The MPL tells us that in this case $S = P$, $S_0 = Z(P)$ and, since $1 \in S_0$, we conclude that p divides $|S_0| = |Z(P)|$. It follows that the series $Z_i(P)$ is a strictly increasing sequence of subgroups which must terminate in G. This ends the proof.

$*$ *Subgroups and homomorphic images of nilpotent groups of class m are nilpotent of class at most m.*

If $H \leq G$, then evidently $L_i(H) \leq L_i(G)$, for all i; it follows that $L_m(G) = 1$ implies

$L_m(H) = 1$. As to homomorphic images, part (3) in the commutator section and induction yield $f(L_j(G)) = L_j(f(G))$, for all j. Thus $L_m(G) = 1$ implies $L_m(f(G)) = f(L_m(G)) = f(1) = 1$, for any homomorphism f.

$*$ *If G is nilpotent and H is a subgroup of G, then H is a proper subgroup of its normalizer in G.*

We prove this by induction on the nilpotence class of G. Assume that the result is true for all groups of nilpotence class $m-1$ or less. Let G have nilpotence class m, and H be a proper subgroup of G with $N_G(H) = H < G$. Since $1 \neq Z(G)$, $\bar{G} = G/Z(G)$ is nilpotent of class at most $m-1$. Evidently $Z(G)$ normalizes (in fact it centralizes) H and therefore $Z(G) \leq N_G(H) = H$. By the inductive assumption $\bar{H} < N_{\bar{G}}(\bar{H}) = \overline{N_G(H)}$. It follows that $H < N_G(H)$, a contradiction.

Before we state and prove the next result, we observe that if A and B are groups, then $Z(A \times B) = Z(A) \times Z(B)$. [This is not hard to verify. Clearly $Z(A) \leq Z(A \times B)$, and analogously for B, thus $Z(A) \times Z(B) \leq Z(A \times B)$. If $ab \in Z(A \times B)$ and $\alpha \in A$, then $1 = [\alpha, ab] = \alpha ab \alpha^{-1} b^{-1} a^{-1} = [\alpha, a]$, which shows that $a \in Z(A)$; similarly $b \in Z(B)$. Thus $Z(A \times B) \leq Z(A) \times Z(B)$.]

It is now easy to see that *if A and B are nilpotent groups, then so is $A \times B$*. Indeed, since $(Z_i(A))$ and $(Z_i(B))$ are strictly increasing series in A and B, respectively, then $(Z_i(A \times B)) = (Z_i(A) \times Z_i(B))$ is a strictly increasing series in $A \times B$.

$*$ *A group is nilpotent if and only if it is the direct product of its Sylow subgroups.*

If G is the direct product of its Sylow subgroups, and since each $p-$group is nilpotent, it follows that G is nilpotent. Conversely, let G be nilpotent and P be a Sylow $p-$subgroup of G. By the definition of the direct product, it suffices to show that $P \trianglelefteq G$. If not, then $M = N_G(P) < G$ and $M < N_G(M)$, by a previous result. But Sylow's theorem tells us that P is the unique Sylow $p-$subgroup in $N_G(P)$, and therefore P is characteristic in $N_G(P) = M$, which is in turn normal in $N_G(M)$; it follows that P is normal in $N_G(M)$. We conclude that $N_G(M) \leq M = N_G(P)$, a contradiction. This ends the proof. !!!Define Fitting sgr here. Define Frattini sgr, show it is the sgr of nongenerators, show it is nilpotent using Frattinis argument. Examine Frattini for p-grps. Prove Burnside's basis thm. !!!Include Hall's anzahl theorems here

Semidirect products

Let G be a group. If G has a normal subgroup N and a subgroup H such that $G = NH$ and $N \cap H = 1$, we call G the *semidirect product* of N by H. Subgroup H is called a *complement* of N in G.

Here are a few basic properties of the semidirect product that are easy to verify:

$*$ *Let G be the semidirect product of N by H.*

(1) If H is also normal in G, then $G = N \times H$.

(2) $H \cong G/N$, and $|G| = |N||H|$.

(3) Any element x of G can be written uniquely as $x = nh$, for $n \in N$ and $h \in H$. (We call $x = nh$ the canonical expression of x, and n and h the canonical components of x.)

(4) If $x_1 = n_1h_1$ and $x_2 = n_2h_2$ are canonical expressions for x_1 and x_2, then $x_1x_2 =$

$(n_1h_1n_2h_1^{-1})(h_1h_2)$ *is the canonical expression of* x_1x_2.

(5) Each $h \in H$ *induces an automorphism* $n \to hnh^{-1}$ *of* N *by conjugation. The map* $\alpha : H \to Aut(N)$ *that sends* h *to* $n \to hnh^{-1}$ *is a group homomorphism. If* $x_1 = n_1h_1$ *and* $x_2 = n_2h_2$ *are canonical expressions, then* $x_1x_2 = (n_1\alpha(h_1)(n_2))(h_1h_2)$ *is the canonical expression of* x_1x_2.

(6) $G = N \times H$ *if and only if* α *is the trivial homomorphism that maps* H *into the identity automorphism of* N.

(7) If α *is nontrivial, then* G *is non-Abelian.*

Indeed, (1) is immediate, and (2) follows from the first isomorphism theorem. As to (3), $x = n_1h_1 = n_2h_2$ implies $n_2^{-1}n_1 = h_2h_1^{-1} \in H \cap N = 1$. Part (4) is readily verified using normality of N. Part (5) is a retelling of (4) when viewing H as conjugations on N. Lastly, (6) and (7) are very easy to see.

We thus conclude that the semidirect product G is determined by N and H and the conjugations induced by elements of H on N.

Motivated by part (5) above, let N and H be groups, and $\alpha : H \to Aut(N)$ be a homomorphism. We view elements of H as automorphisms of N, by identifying h with $\alpha(h)$; such an identification is helpful even when the representation α is not injective.

Let S be the set product $N \times H$. Define a binary operation on S by

$$(n_1, h_1)(n_2, h_2) = (n_1\alpha(h_1)(n_2), h_1h_2) \; n_1, n_2 \in N; \; h_1, h_2 \in H.$$

We call S the *external semidirect product* of N by H with respect to α. Whenever a need for explicitness arises, we denote this semidirect product by $S(N, H, \alpha)$. Observe that when α is the trivial homomorphism (that is, when $\alpha(A) = 1$) the semidirect product is just the direct product of N and H.

$*$ *The semidirect product S has the following properties:*

(1) S is a group.

(2) The maps $i_N : n \to (n, 1)$ and $i_H : h \to (1, h)$ are injective homomorphisms.

(3) The subgroup $i_N(N)$ is normal in S, and S is the semidirect product of $i_N(N)$ by $i_H(H)$.

(4) $(n, 1)^{(1,h)} = (\alpha(h)(n), 1)$ for all $n \in N$ and $h \in H$.

Associativity is streightforwardly verified. The identity is $(1, 1)$. The inverse of (n, h) is $(\alpha(h^{-1})(n^{-1}), h^{-1})$. This proves (1). Part (2) is immediate. To check part (3) observe that $(n, 1)^{(m,h)} = (m, h)(n, 1)(m, h)^{-1}$ has a 1 in the second component and is therefore in $i_N(N)$. That $i_N(N) \cap i_H(H) = (1, 1)$ is immediate, while $i_N(N)i_H(H) = S$ follows from considerations of cardinality. As to (4), $(n, 1)^{(1,h)} = (1, h)(n, 1)(1, h)^{-1} = (\alpha(h)(n), h)(1, h^{-1}) = (\alpha(h)(n), 1)$, which shows that conjugation on $i_N(N)$ induced by $i_H(H)$ in the group S corresponds to the action of H as a group of automorphisms of N given by $\alpha : H \to Aut(N)$.

Group G is an *extension* of a group X by a group Y if there exists $H \trianglelefteq G$ with $H \cong X$ and $G/H \cong Y$. The extension is said to *split* if H has a complement K in G; in this case we say that G *splits* over H, or that G is a *split extension* of H by K.

The next result shows that the split extensions of H by K are precisely the semidirect products with K acting on H by conjugation.

$*$ *Let H and K be subgroups of G. Then $G \cong S(H, K, \alpha)$, with $\alpha(k)(h) = khk^{-1}$ if and only if G is a split extension of H by K.*

If $G \cong S(H, K, \alpha)$ by (3) of the previous result $i_H(H) \trianglelefteq S(H, K, \alpha)$, $i_K(K)$ is a complement of $i_H(H)$ in $S(H, K, \alpha)$ and, by the second isomorphism theorem, $S(H, K, \alpha)/i_H(H) \cong i_K(K)$. This shows that $G \cong S(H, K, \alpha)$ is a split extension of H by K. (We did not use the fact that α is conjugation for this implication.)

Assume now that G is a split extension of H by K. Consider $S(H, K, \alpha)$ with $\alpha(k) = khk^{-1}$. Observe that $S(H, K, \alpha) \cong G$, by mapping (h, k) to hk. The map $f((h, k)) = hk$ is an injective homomorphism, since $f((h_1, k_1)(h_2, k_2)) = f((h_1 k_1 h_2 k_1^{-1}, k_1 k_2)) = h_1 k_1 h_2 k_1^{-1} k_1 k_2 = (h_1 k_1)(h_2 k_2) = f((h_1, k_1) f((h_2, k_2))$, and $hk = 1$ implies $h, k \in H \cap K = 1$. This ends the proof. !!!A little more on semidirects, like N by cyclic H. Do all G of order 16 or less as semis

A nice result on split extensions appears below. It tells us that the question of split extensions of an Abelian normal $p-$subgroup of a group G is settled within a Sylow $p-$subgroup of G.

Theorem (Gaschütz)

Let $V \leq P$ be subgroups of G with V Abelian normal in G and P a Sylow $p-$subgroup of G. Then G splits over V if and only if P splits over V.

Proof: *(following Ashbacher*, minus misprints*)*

If H is a complement of V in G, then $P = P \cap G = P \cap (VH) = V(P \cap H)$, and $V \cap (P \cap H) \leq V \cap H = 1$ which shows that $P \cap H$ is a complement of V in P.

Conversely, suppose Q is a complement to V in P. Denote by $\bar{G}$ the factor group G/V. Let X be a set of coset representatives of V in G. Denote by x_a the element of X representing coset a of $\bar{G}$. We have

$$x_a x_b = x_{ab}\gamma(a,b), \text{ for all } a,b \in \bar{G}, \text{ and some } \gamma(a,b) \in V. \ (1)$$

[Our goal is to select X in such a way that in (1) we have $\gamma(a,b) = 1$, for all $a,b \in \bar{G}$.]

Using associativity in G and $\bar{G}$ we have

$x_{abc}\gamma(a,bc)\gamma(b,c) = x_a x_{bc}\gamma(b,c) = x_a(x_b x_c) = (x_a x_b)x_c = x_{ab}\gamma(a,b)x_c = x_{ab}x_c\gamma(a,b)^{x_c^{-1}} = x_{abc}\gamma(ab,c)\gamma(a,b)^{x_c^{-1}}$.

[The above equations are best read by starting in the middle and moving toward the ends.] Muliplying the equations through by x_{abc}^{-1} we obtain

$$\gamma(ab,c)\gamma(a,b)^{x_c^{-1}} = \gamma(a,bc)\gamma(b,c), \text{ for all } a,b,c \in \bar{G}. \ (2)$$

Since $V \leq P$, a coset of P in G is union of cosets of V in G. We can therefore select $X = QY$, where Y is a set of coset representatives of P in G. [Notice that elements of Q are coset representatives of V in P; indeed, $q_1V = q_2V$ implies $q_2^{-1}q_1 \in V \cap Q = 1$, and $VQ = P$ insures that all of P is covered. It is thence clear that $Q \cong Q/V = \bar{Q} = \bar{P} = P/V$.] For $q \in Q$ we write $\bar{q} = qV \in \bar{Q}$. Then for $q \in Q$ and $a \in \bar{G}$ we have $x_{\bar{q}a} = qx_a \in QY$, and therefore we conclude that

$$x_q = q, \text{ and } \gamma(\bar{q},a) = 1, \text{ for all } q \in Q \text{ and } a \in \bar{G}. \ (3)$$

By (2) and (3) we have

$$\gamma(\bar{q}b,c) = \gamma(b,c), \text{ for all } b,c \in \bar{G} \text{ and } q \in Q. \ (4)$$

For $c \in \bar{G}$, define $\beta(c) = \prod_{y\in Y}\gamma(\bar{y},c)$. Observe that

$$\beta(c) = \prod_{y\in Y}\gamma(\bar{y}b,c) \text{ for all } b,c \in \bar{G}. \ (5)$$

[Indeed, the fact that $\{\bar{y} : y \in Y\}$ is a set of coset representatives of $\bar{P}$ in $\bar{G}$ immediately implies that $\{\bar{y}b : y \in Y\}$ is also a set of coset representatives of $\bar{P}$ in $\bar{G}$, for any $b \in \bar{G}$. Therefore, elements $\gamma(\bar{y}, c)$ with $y \in Y$, are the same as $\gamma(\bar{y}b, c)$ with $y \in Y$, up to a possible reordering; this explains (5).]

Using (2) and commutativity in V we obtain

$$(\prod_{y\in Y}\gamma(\bar{y}b,c))(\prod_{y\in Y}\gamma(\bar{y},b))^{x_c^{-1}} = (\prod_{y\in Y}\gamma(\bar{y},bc))(\prod_{y\in Y}\gamma(b,c)).$$

Appealing to (5) this yields

$$\beta(c)\beta(b)^{x_c^{-1}} = \beta(bc)\gamma(b,c)^m, \text{ for all } b, c \in \bar{G} \ (6)$$

where $m = |G : P|$. Since P is a Sylow $p-$subgroup of G, $(m, p) = 1$; therefore m is invertible modulo $|V|$. Whence we can define $\alpha(c) = \beta(c)^{-m^{-1}}$, for $c \in \bar{G}$. Taking the $(-m^{-1})^{th}$ power of (6) we obtain

$$\alpha(c)\alpha(b)^{x_c^{-1}} = \alpha(bc)\gamma(b,c)^{-1}, \text{ for all } b, c \in \bar{G}. \ (7)$$

Define $y_a = x_a\alpha(a)$, for all $a \in \bar{G}$, and let $H = \{y_a : a \in \bar{G}\}$. We show that H is a complement of V in G. It suffices to show that $y_by_c = y_{bc}$, for all $b, c \in \bar{G}$. But

$$y_by_c = x_b\alpha(b)x_c\alpha(c) = x_bx_c\alpha(b)^{x_c^{-1}}\alpha(c) = x_{bc}\gamma(b,c)\alpha(b)^{x_c^{-1}}\alpha(c) =$$

$$y_{bc}\alpha(bc)^{-1}\gamma(b,c)\alpha(b)^{x_c^{-1}}\alpha(c) = y_{bc}.$$

The last sign of equality follows from (7) and commutativity in V. This ends the proof.

The special case $V = P$ in Gaschütz's theorem allows us to conclute that *Any Abelian normal Sylow p-subgroup of G has a complement in G.* Equivalently, a group splits over any of its Abelian normal Sylow $p-$subgroups. This will prove helpful in the proof of the Schur-Zassenhaus theorem given below.

The Frattini argument

If $N \trianglelefteq G$, and P is a Sylow subgroup of N, then $G = N_G(P)N$.

Indeed, since $N \trianglelefteq G$ we have $P^x \leq N$, for all $x \in G$. For $x \in G$, by Sylow's Theorem $nP^xn^{-1} = P$, for some $n \in N$. Thus $nxP(nx)^{-1} = P$, which shows that $nx \in N_G(P)$. It follows that $(nx)^{-1} = x^{-1}n^{-1} \in N_G(P)$, or $x^{-1} \in N_G(P)n$; this proves that $G = N_G(P)N$.

A subgroup H of a group G is called a *Hall subgroup* if $|H|$ and $|G : H|$ are relatively prime (or *coprime*, for short).

Theorem (Schur-Zassenhaus)

Any normal Hall subgroup has a complement.

Proof: Let N be a Hall subgroup of group G. Denote $|G : N|$ by n. If G has a subgroup K of order n, then K is a complement of N in G, since necessarily $N \cap K = 1$ (by the coprimality of $|N|$ and n) and $NK = G$ (since $|G| = |N||K| = |NK|$). It suffices, therefore, to prove that G contains a subgroup of order n. In what follows we shall assume by induction that the statement of the Theorem is true in all groups of order less than $|G|$.

Let P be a Sylow subgroup of N. By the Frattini argument, we have $G = N_G(P)N$. Observe that $N_N(P) = N_G(P) \cap N$ is normal in $N_G(P)$, and $G/N = N_G(P)N/N \cong N_G(P)/(N_G(P) \cap N) \cong N_G(P)/N_N(P)$ by the second isomorphism theorem. Therefore $|N_G(P) : N_N(P)| = n$, and since $|N_N(P)|$ divides $|N|$, it follows that $N_N(P)$ is a normal Hall subgroup of $N_G(P)$. If $N_G(P) < G$, then by induction $N_G(P)$, and hence G, has a subgroup of order n. We may, therefore, assume that $N_G(P) = G$ or, equivalently, that

$P \trianglelefteq G$.

Suppose that $P \triangleleft N$. By the correspondence theorem we have $N/P \trianglelefteq G/P$, and $|G/P : N/P| = |G : N| = n$. Since $|N/P|$ divides $|N|$ and $|G/P| < |G|$, by induction G/P has a subgroup of order n. This subgroup must be of the form L/P where $P \triangleleft L \leq G$. Observe that $|L| = n|P| < n|N| = |G|$ which implies $L < G$. Since $|P|$ and $|L/P|$ are coprime, by induction we know that L, and hence G, has a subgroup of order n.

Assume now that $N = P$. Being a $p-$group and a Hall subgroup N is necessarily a Sylow subgroup of G. Suppose, furthermore, that N in non-Abelian. Let $Z = Z(N)$; then $1 < Z \triangleleft N$, since N is a $p-$group. Note that since Z is characteristic in N, and $N \trianglelefteq G$, it follows that $Z \triangleleft G$. By the correspondence theorem G/Z has a normal subgroup N/Z of index n. Thus by induction, G/Z has a subgroup of order n of the form L/Z where $Z \triangleleft L \leq G$. But $|L| = n|Z| < n|N| = |G|$, which informs us that $L < G$. Here $|Z|$ and $|L/Z|$ are coprime, and therefore L, and hence G, has a subgroup of order n.

Lastly, assume that $N = P$, and N is Abelian. Gaschütz's theorem insures a complement to N in G in this case. This ends the proof.

Here is another *gem.*

Theorem (Philip Hall)

If G is a solvable group of order mn, with m and n coprime, then

(i) G has a subgroup of order m.

(ii) Any two subgroups of order m are conjugate in G.

(iii) Any subgroup of G whose order divides m is contained in a subgroup of order m.

[The Theorem states, in other words, that solvable groups contain Hall subgroups of all orders, that any two Hall subgroups of the same order are conjugate, and that any subgroup whose order divides the order of a Hall subgroup is necessarily included in such a Hall subgroup. Since Sylow subgroups are Hall subgroups we view Hall's Theorem as an extension of Sylow's Theorem to solvable groups.]

Proof: Assume by induction that the Theorem is true for any group of order less than $|G|$. Let N be a minimal normal subgroup of G. We know that N is an elementary Abelian $p-$group, for some prime p that divides $|G| = mn$. Since m and n are coprime, p divides exactly one of m or n.

1. If p divides m, then $|G/N| = (m/|N|)n$ is a product of coprime integers $m/|N|$ and n. By induction, therefore, G/N has a subgroup H/N of order $m/|N|$; it follows that subgroup H is a subgroup of order m in G.

Observe that since p divides m (but not n), the normal subgroup N is contained in every Sylow $p-$subgroup of G and is, therefore, contained in every subgroup of order m in G. Thus, if H_1 and H_2 are two subgroups of order m in G, then H_1/N and H_2/N are, by induction, conjugate subgroups of G/N. This immediately implies that H_1 and H_2 are conjugate in G. [Specifically, if $H_2/N = (H_1/N)^{gN}$, then $H_2 = H_1^g$.]

Let K be a subgroup of G whose order $k = |K|$ divides m. Then KN/N is a subgroup of G/N whose order divides both k (since $|KN/N| = |K/(N \cap K)|$) and $|G/N| = (m/|N|)n$. It follows that the order of KN/N divides $m/|N|$ and KN/N is by induction included is a subgroup H/N of order $m/|N|$ of G/N. It follows that $KN \leq H$, and hence $K \leq H$. Clearly H has order $(m/|N|)|N| = m$.

2. Suppose now that p divides n. Since $|G/N| = m(n/|N|)$ by induction G/N has a subgroup K/N of order m. Note that $|K| = m|N|$ is a product of coprime integers m and $|N|$.

Case 2(a). Assume that $m|N| < |G|$. Thus $K < G$. By induction K, and hence G, has a subgroup of order m.

Let H_1 and H_2 be subgroups of order m in G. Note that $|H_iN/N| = |H_i/(H_i \cap N)| = |H_i| = m$, and by induction H_1N/N and H_2H/N are conjugate in G/N. Therefore $H_2N = (H_1N)^g$ for some $g \in G$. It follows that H_1^g and H_2 are subgroups of H_2N and, since $|H_2N| = m|N| < |G|$, by induction they are conjugate in H_2N. We now see that H_1 and H_2 are conjugate in G.

Let M be a subgroup of G whose order divides m. Since $|MN/N| = |M/(M \cap N)| = |M|$, by induction there exists a subgroup H/N of order m such that $MN/N \leq H/N$; observe that H has order $m|N| < |G|$. It follows that $MN \leq H$, thus $M \leq H$, and by induction M is included in a subgroup of order m of H, and hence of G.

Case 2(b) Assume that $m|N| = |G|$. It follows that N is an elementary Abelian minimal normal Sylow $p-$subgroup of G. We write $n = |N| = p^r$, and $|G| = mp^r$, with m and p coprime. Let K/N be a minimal normal subgroup of G/N. We know that K/N is elementary Abelian of order q^s, for some prime $q \neq p$. Thus $|K| = p^r q^s$, and $K \trianglelefteq G$. Let S be a Sylow $q-$subgroup of K.

Since $K \trianglelefteq G$, the Frattini argument gives $G = KN_G(S)$. Clearly $N_K(S) = N_G(S) \cap K$. Therefore,

$$G/K = (KN_G(S))/K \cong N_G(S)/(K \cap N_G(S)) = N_G(S)/N_K(S).$$

Notice that $K = NS$, and since $S \leq N_K(S) \leq K$, we also have $K = NN_K(S)$. This gives $|K| = |NN_K(S)| = |N||N_K(S)|/|N \cap N_K(S)|$ and therefore

$$|N_G(S)| = \frac{|G||N_K(S)|}{|K|} = \frac{|G|}{|N|}|N \cap N_K(S)| = m|N \cap N_K(S)|.$$

Assume that $N \cap N_K(S) = 1$.

It follows from the above that $N_G(S)$ is a subgroup of order m of G.

Let H be a subgroup of order m in G. We show that H is conjugate to $N_G(S)$. Since $|KH| = |G| = mp^r$ and $|K| = p^r q^s$ it follows that $H \cap K$ is a Sylow $q-$subgroup of K. By Sylow's Theorem we have $H \cap K = S^g$ for some $g \in G$. Whence $N_G(H \cap K) = N_G(S)^g$, and $|N_G(H \cap K)| = |N_G(S)^g| = m$. But $H \leq N_G(H \cap K)$, since $(H \cap K) \trianglelefteq H$, which shows that $H = N_G(H \cap K)$. We conclude that H and $N_G(S)$ are conjugate.

Let T be a subgroup of G whose order divides m. Let $R = (NT) \cap N_G(S)$. Then $|R| = \frac{|NT||N_G(S)|}{|NTN_G(S)|} = \frac{p^r|T|m}{p^r m} = |T|$. It follows that R and T are conjugate in NT, since $|NT| = |T|p^r$ with $|T|$ and p^r coprime. Thus $T = R^g$ for some $g \in G$. Since $R \leq N_G(S)$, $T \leq N_G(S)^g$.

Assume that $N \cap N_K(S)| \neq 1$.

Let $x \in N \cap N_K(S)$. Since N is Abelian and $x \in N$, $[x, N] = 1$. Furthermore $(xsx^{-1})s^{-1} \in S$ since $x \in N_K(S)$, but also $x(sx^{-1}s^{-1}) \in N$ since $x \in N$ and N is normal in G. Thus $xsx^{-1}s^{-1} \in S \cap N = 1$. We conclude that $[x, S] = 1$, and therefore that $[x, NS] = [x, K] = 1$. Therefore $x \in Z(K)$, which shows that $N \cap N_K(S) \leq Z(K)$. But $Z(K)$ is characteristic in K, and $K \trianglelefteq G$, thus $Z(K) \trianglelefteq G$. By minimality of N we have $N \leq Z(K)$. It follows that both S and N are in $N_K(S)$, and hence $K = NS = N_K(S)$, thus $S \trianglelefteq K$. As a normal Sylow $q-$subgroup of K, S is characteristic in K and thus normal in G.

Consider G/S. Since $|G/S| = (m/q^s)p^r$ is a product of coprime integers m/q^s and p^s, by induction G/S has a subgroup H/S of order m/q^s; it follows that subgroup H is a subgroup of order m in G.

Observe that since q^s divides m (but not p^r), the normal subgroup S is contained in every Sylow $q-$subgroup of G and, therefore, in every subgroup of order m in G. Thus, if H_1 and H_2 are two subgroups of order m in G, then H_1/S and H_2/S are, by induction, conjugate subgroups of G/S. This immediately implies that preimages H_1 and H_2 are conjugate in G.

Let W be a subgroup of G whose order divides m. Then WS/S is a subgroup of G/S whose order divides both $|W|$ and $|G/S| = (m/q^s)p^r$. It follows that the order of WS/S divides m/q^s and WS/S is by induction included is a subgroup H/S of order m/q^s of G/S. Consequently $WS \leq H$, and hence $W \leq H$. Clearly H has order $(m/q^s)q^s = m$. This completes the proof.

!!!Prove Frob conj for solvable grps. Discuss general case.